PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : A63F 9/24, 9/22 // G06F 161:00, G07F 17/32 — A1

(11) International Publication Number: **WO 98/40140**

(43) International Publication Date: 17 September 1998 (17.09.98)

(21) International Application Number: PCT/AU98/00152

(22) International Filing Date: 10 March 1998 (10.03.98)

(30) Priority Data:
PO 5543 10 March 1997 (10.03.97) AU

(71) Applicant *(for all designated States except US)*: ARISTOCRAT LEISURE INDUSTRIES PTY. LTD. [AU/AU]; 85–113 Dunning Avenue, Rosebery, NSW 2018 (AU).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: MUIR, Robert, Linley [AU/AU]; 7/6 Benton Avenue, Artarmon, NSW 2064 (AU).

(74) Agent: F.B. RICE & CO.; 605 Darling Street, Balmain, NSW 2041 (AU).

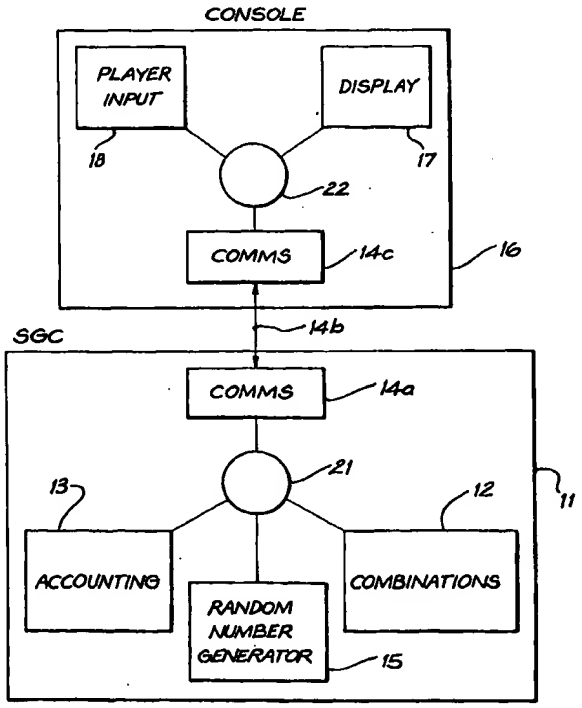
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: PERSONAL GAMING SYSTEM

(57) Abstract

A gaming console and a gaming console controller are provided where the controller includes a secure credit storage, a secure processing device, a secure program storage and secure communications, such that the control device may perform all of the essential secure functions of a gaming console. The control means may be removable from the console and personal to the user or may be permanently fixed into the console.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Personal gaming system

Introduction

The present invention relates generally to the field of gaming machines and in particular, the invention provides a device for controlling gaming machines which simplifies the security arrangements in both conventional and portable gaming machines.

Background of the invention

A traditional gaming machine is a self contained unit containing a player interface and microprocessor control logic and software games. Several types are popular, including the traditional upright slot machine, slant top, and bar top slot machines.

Features typical of these machines are:

- These machines are physically large and heavy.
- They are fixed in place and cannot easily be moved. Some units must be fixed in place to prevent serious personal injury if they fell on a person, due to their weight. Security of the money inside is also maintained by their being fixed in place.
- The security provided by the machines is primarily physical, such as locks and doors, backed by electronic sensors, and auditing recorded meter values (records of cash in/out etc). In addition, the machines are usually used in full view of the operators, preventing any serious attempt by the public at stealing from them.
- Security is required to prevent tampering with the machine by either casino staff or customers. Physical security involves physical locks and electronic sensors, both on the main chassis and internal logic cage. Auditing of metered values, including cash in and cash out, can provide further checking of the integrity of operation. The logic cage is an internal high security cage containing the highly sensitive CPU, game storage memory, security control logic, and any other components that may affect the game outcome.
- Machines must be available to government inspectors, who can check that the machines have not been illegally modified to cheat the public.

Due to these features and gaming laws, gaming machines are restricted to carefully prescribed venues, including casinos and certain clubs.

Security considerations mandate the use of a logic cage enclosing the sensitive components. Due to practical considerations (an enclosure is

required to physically hold all the assemblies) it also usually holds most of the rest of the logic in the machine. For example the music generation circuit may not be considered as sensitive but is typically within the logic cage.

Currently, gaming toys such as those made by Radica:™, allow "pretend" gambling, where no money can be won or lost. Imaginary money is gambled, and typically, when the credit level reaches zero, more credits are automatically added.

Many governments require gaming machines to be monitored to control illegal gaming and ensure taxes are collected. However this is difficult in many underdeveloped areas in the world as poor communications limit the areas and reliability of on-line (telephone) monitoring.

The player interacts with the gaming machine via a number of means:

- Graphics are displayed to the player, typically on a video display or stepper reels.
- Sound effects are output from an audio speaker.
- The player controls the game through various means, including but not limited to, a handle, buttons, and touch screen.

Throughout this specification, the following definitions will apply:

- A **casino** is used to refer not only to a traditional casino, but a more general financial institution that backs the games played with money. A real physical casino in the traditional sense may not exist, and such an institution more closely resembles a bank. For the purpose of this patent a traditional casino, pub, hotel, aircraft, or ship, etc, can also be considered as a casino.
- **Game data** refers to that data on a console that is required to provide a user interface to the player, including graphics, sound, and code (but not combinations).
- The **combinations** of a game describe the mathematical structure of the game and define all possible games, including the winning patterns and the payouts associated with each. From the combinations the game statistics are determined, including the theoretical return to the player.
- A **game outcome** is the result of a game including the amount returned to the player in a winning game and the code defining the image displayed to the user to indicate the game result. In the case of a game console (as

opposed to a control device) game outcome also includes the actual display image displayed at the end of the game.

- **Credits** represent money in the gaming environment. The casino interchanges money and credits for the player, although credits may be exchanged for other types of value (gifts, etc).
- **SAM** refers to Secure Access Means.
- **SPM** refers to Secure Processing Means.
- **SSM** refers to Secure Storage Means.
- **SGC** refers to Secure Gaming Controller, which may include an SPM an SSM and secure communication means.
- A **distributed gaming** system is one in which the players user interface is physically separated from the game outcome logic. Internet gaming is a prime example.

Summary of the invention

According to a first aspect, the present invention provides a game console secure control device implemented as a single secure integrated control circuit arranged to perform game outcome determination of a game played on a game console to which the control device is connected, the integrated control circuit having input/output means to allow communications with the console.

According to a second aspect, the present invention provides a game console secure control device implemented as a secure single integrated control circuit arranged to perform game outcome determination of a game played on a game console to which the control device is connected, the integrated control circuit having data storage means and input/output means , the data storage means, including game outcome storage means whereby the control device is preprogrammed with a set of game outcomes in the game outcome storage means and when a player playing the connected console initiates a game, a game outcome is determined from the set of game outcomes and the input/output means being arranged to allow communication with the console.

Preferably the secure control means is a data processing means having associated program storage means, preferably also the program storage means includes a control program to control the playing of games on a gaming machine into which the control device is connected.

The control device preferably also includes data storage means, which in some embodiments includes credit storage means, enabling the control device to be preprogrammed with a credit amount. In use a wager would then be deducted from the credit amount in the credit storage means, and in the event that the generated game outcome is a winning outcome, a prize value is credited to the credit value.

In other embodiments the secure data storage means is provided externally to the control device, and the input/output means is arranged to provide secure communications with the data storage means such that a credit balance associated with the player playing the game may be stored in the data storage means. In a further embodiment the external secure data storage means may instead or additionally hold a set of game outcomes, a set of random seed values, a set of game combinations, or programs associated with the playing of games on the console. In the case of outcomes, seeds, combinations, or programs, when a player playing the connected console initiates a game, a game outcome is determined from the set of game outcomes or a seed value is used to generate a random outcome and or one of the sets of combinations or programs is used to determine the outcome or outcome indication on the console.

Preferably the control device includes credit adjustment means arranged to adjust the credit balance associated with a player playing the game, to deduct a wager from the credit balance and, when a prize value is awarded as a result of the game, crediting the prize value to the credit balance. In one embodiment the credit adjustment means is arranged to read the credit balance, calculate a new balance and write the new balance to the data storage means, while in another embodiment the credit adjustment means is arranged to communicate a credit balance adjustment amount to the data storage means, and the data storage means is arranged to calculate and store a new balance.

Preferably the secure means is implemented as a secure integrated circuit or module.

According to a third aspect, the present invention provides a game console including outcome indication means and user input means, control means arranged to control the non-secure functions of the game console, and secure control device interface means to provide communication between the secure control device and the control means whereby, when the secure

control device is present and the game console is in use, a game initiating input made by a player to initiate a game causes a game outcome to be determined by the secure control device and communicated to the console, the game outcome causing an outcome indication selected from a set of possible indications to be exhibited by the outcome indication means.

According to a fourth aspect, the present invention provides a method of verifying authorisation of a host device or system to use a program or preprogrammed device having a secure function which it performs when stored or located in or connected to the host device or system wherein the host device or system is provided with a secure authorisation device and the program or programmed device interrogates the authorisation device by transmitting or otherwise communicating a message to the authorisation device and receiving a response from the authorisation device, determining, if the response corresponds with the original message, the authorisation device being passed as authentic and the program or programmed device being permitted proceed to perform its secure function only if this correspondence exists.

In gaming applications, the authentication device will be located in the console and the control device authenticates the console by detecting the authentication device.

Preferably, the control device is implemented using known security technology such as smartcard technology, and may for example, use a smartcard or smartcard chip or alternatively, in a different card arrangement such as a PCMCIA card, or a custom card arrangement. Arrangements are also proposed in which a smartcard chip is mounted into a floppy disk casing together with a magnetic interface for communication with the heads of a floppy disk drive. The control device may also be a fixed function logic circuit. Game outcome indication may be voice messages, video displays or other suitable indications, but in the preferred embodiment, output indications will be displayed on a video display device. However, other embodiments may employ non-video display devices such as spinning reels. In some embodiments, at least some game outcomes will have associated with them, a plurality of possible outcome indications, or displays, of equal prize value and the game console or control device control program will select one display from the set of displays of equal value. The selection may be made on a sequential or random basis.

In one possible embodiment of the invention, the game console is capable of playing a plurality of different games and the outcome indication means will display an output indication from a set of possible indications for the game in play.

Preferably, the game console control device is arranged to control each of a plurality of different types of game console and a common game is available for play on all of the console types, although, the outcome indications may differ in detail from one console type to another (eg, between a hand held gaming console with a small LCD display and a traditional upright gaming console with high resolution video display.

The program and data memory of the control device may optionally include code and data for generating user interface displays on a display device in the game console and for monitoring user input devices of the game console or alternatively, the programs, screen definitions etc may reside in non-secure memory in the game console, external to the control device, or may be downloaded from the control device to the console.

The control device may be a removable device carried by the user and inserted into a game console of choice by the user. Alternatively, the control device may be permanently or semi-permanently mounted in the console in a location that is not user accessible. Consoles may also be of different styles such as, for example, hand held devices or traditional free standing Electronic Gaming Machines (EGMs).

The game console may be a permanently or semi-permanently located console housing similar in function and appearance to a standard slot machine or may be a portable or hand held unit. The game console may also be a personal computer with a suitable interface to receive the control device or a video game controller connected to a television.

Random number generation within the control device may either be by way of a random number generating circuit employing, for example, a noise generating circuit, or relying on the randomness of user input timing. Alternatively, the control device may employ a pseudo-random number generating algorithm. In the case of a random number generating algorithm, one or more seeds may optionally be loaded into the control device periodically (eg when performing a credit transaction) to break the pseudo-random sequence.

According to a fifth aspect the present invention provides a game console secure data storage means implemented as a secure single integrated memory circuit arranged to be connected externally to a secure control device, the data storage means including game outcome storage means whereby the data storage means is preprogrammed with a set of game outcomes, the data storage means having input/output means arranged to provide secure communication with the integrated control circuit, such that when a player playing the connected console initiates a game, a game outcome is determined from the set of game outcomes.

In one embodiment the data storage means includes credit balance storage means whereby a credit balance associated with the player playing the game is stored in the data storage means.

In various embodiments the secure data storage means may be permanently or semi-permanently connected to the console, or may be removably connectable to the console, whereby the player may possess the data storage device and insert it into a console of choice.

The secure communication with the secure control device may be by way of cryptographic security means. or physical security means.

The secure control device includes credit adjustment means arranged to adjust the credit balance associated with a player playing the game to account for any wager bet and prize value won as a result of the game. The credit adjustment may be achieved by various methods, including:

1. Deducting a wager value from the credit balance at the commencement of the game and if a prize is awarded adding the prize value to the credit balance after the outcome is determined.

2. Reading the credit balance, calculating a new balance and writing the new balance to the data storage means after the outcome is determined.

3. Communicating a credit balance adjustment amount to the data storage means after the outcome is determined, and calculating and storing a new balance within the data storage means.

Brief Description of the Drawings

Embodiments of the invention will now be described by way of example, with reference to the accompanying drawings in which:

Figure 1 shows a block diagram of an architecture for one embodiment of the invention;

Figure 2 shows a flow chart for an initialisation routine for the embodiment of Figure 1;

Figure 3 shows a block diagram for an Account Register sub-system, employed in embodiments of the invention;

Figure 4 shows a flow chart for a game play sequence employed in embodiments of the invention;

Figure 5 shows a diagram of funds transfer paths which can be employed with certain embodiments of the present invention;

Figure 6 shows a block diagram of a console embodying the present invention and illustrating the use of a co-operating license chip.

Detailed Description of the Preferred Embodiments

Embodiments of the invention form part of a system which will include several parts that together comprise a playable gaming system:

- An SGC on which the secure aspects of a gaming machine are run. The SGC may independently communicate with other systems for the transfer of credits.
- A console that presents to the player a user interface and runs those parts of the game system that are not required to be secure. In some implementations the console may be integrated with the SGC, for example a smartcard with built-in LCD display and buttons.
- A casino that finances games played on the gaming system.
- Communications between SGC and casino.
- The SAM provides secure access to the SSM.
- This secure game controller is comprised of the SPM and SSM connected via secure communications. The SSM holds data on the player's account, including the amount of credits available, accounting information as required for auditing and optionally combinations to be used by the SPM to play the game. The SPM implements the gaming application and stores accounting information as required for auditing.
- A SAM may be used to securely read and update the SSM, and keeps accounting information as required for auditing. It may provide on-line or off-line communications between the SSM and the casino.
- Two implementations are described:
    - A single smartcard integrating SSM and SPM.
    - Two smartcards, one implementing the SSM and the other implementing the SPM.

References to the SGC in are also intended in some cases to apply equally to the SPM and/or SSM and/or SAM. In the interests of clarity only the SGC is referred and the exact meaning depends on context.

In the preferred implementation, the SGC comprising an SPM and SSM, is an ISO 7816 smartcard (or smartcard chip) with embedded microprocessor, ROM, RAM, E^2PROM and communications interface. The SGC implementation could also be a micro-controller or a secure multi-component module, or be composed of a number of physical devices connected via secure communication. Communications with the SGC may be via a direct electrical interface or may be contactless, such as an infra-red or rf link. The key requirement being that it is not possible to determine or influence the internal operation or memory contents of the module, and hence influence the outcome of games or adjust the account.

The console varies depending on the application, some of which are:

- A personal gaming machine comprising of a small hand held console, similar in concept to a "Gameboy™" games console, or "Radica:™" gaming toy into which a SGC is either inserted by the player or embedded by the manufacturer (Gameboy is a trade mark of Nintendo Corporation and Radica is a trade mark of Radica Games Limited).
- A hand held gaming machine for use in a traditional gaming environment with an embedded security device to prevent the machine being removed from the premises, in a manner similar to that used to prevent theft in a shop.
- A traditional gaming machine with enhanced security features provided by an embedded SGC.
- A small gaming machine in which the machine output is in the form of voice and/or sound effects.
- A traditional gaming machine used as the console, with the SGC being carried by the player from machine to machine.
- A new type of gaming machine, such as may be used in Hotel in-room, cafe, pub, or aircraft gaming, where traditional security of the machine is not possible. Security is then provided by the SGC, which may or may not be embedded within the machine.
- Gaming on a home or business computer, with the computer as the console. Credits may be transferred to the smartcard via a

communications link to the casino. The computer may be an Internet terminal and credits transferred via the Internet.

- An SGC that is carried by the player, rather than being embedded within the console, may be used in more than one of the appropriate applications described above. For example the player may have a hand held console, but take the SGC from it and play it in a traditionally styled machine in a casino.
- A plug-in module for a game console (eg Sony Playstation ™ or Nintendo Ultra 64™), containing the game program game data, for the console and the SGC. The module may additionally have a modem for communication as will be described later.

An SGC that is carried by the player, rather than being embedded within the console, may be used in more than one of the appropriate applications described above. For example the player may have a hand held console, but take the SGC from it and play it in a traditionally styled machine in a casino.

The complete gaming machine then comprises of two parts, the console and smart card, as shown in Figure 1. The SGC 11 contains at least those components of the game that determine the game payout. In a traditional machine the high security logic cage protects these, and other elements against tampering. Each of the following components should be absolutely secure to prevent tampering, and are therefore located within the SGC 11 although other components of the game may also be included:

- The combinations 12 of the game held in secure memory (SSM) 23.
- Accounting data 13 held in SSM.
- Communications 14a, including means for transfer of credits to and from the smartcard 11.
- The random number generator (RNG) 15 used to determine game outcomes.
- The SGC 11 is managed by a processor 21 which coordinates the other functions of the SGC.

The console 16 provides a user interface to the player for the games running on the SGC 11. The user interface provided by console 16 may include any of the traditional components, including a video display 17, audio output, buttons, handle and touch screen input. When in communication with the casino via optional communications link, the

console 16 may act as the intermediary to transfer credit to the SGC 11. The console may have other communications systems provided via the link to allow it to run distributed games or for the collection of game statistics by a controller. The console 16 is managed by a processor 22 which coordinates the functions of the console.

In one alternative implementation the SGC also contains some or all of the data required by the console to play the game. Currently smartcards do not have much storage capacity, but as this increases it will become feasible to store some or all the game data on a smartcard.

Combinations may be programmed into smartcard ROM, E^2PROM or RAM. Programming combinations into E^2PROM or RAM allows flexibility, with a single masked ROM smartcard being able to be used for many different combinations and hence games. These combinations are loaded into the smartcard either as a once off process during manufacture (ROM or E^2PROM) or later as required by the user (E^2PROM or RAM). Combinations downloaded by the user are secured to prevent tampering, using for example encryption or digital signatures.

Preferably to prevent unauthorised use of the smartcard, players are required to identify themselves to the smartcard in order for it to function, typically using a pin number, password or biometric identification. Multiple accounts (eg. members of a family) may be accessed using a single smartcard and multiple pins, passwords or biometric identification.

Alternate Implementation

In an alternate implementation the secure processing means 21 and SSM functions of the secure gaming controller are split between two physically separate devices communicating via secure communications. Preferably these two devices are smartcards.

The SSM holds the player's account data, including the amount of credit available, accounting information as required for auditing and optionally combinations or code. In an implementation of predetermined outcomes, the SSM may also hold predetermined outcomes. The SPM implements the gaming application and stores accounting information as required for auditing. The SPM 21 also typically implements secure storage 24, to the extent require for operation.

Gambling is enabled when the user connects the SSM to the SPM 21 (in the console). Two methods of gambling and credit transfer are described:

- Credits bet are temporarily transferred from the players SSM to the SSM 24 within the SGC. They are bet on, in one or more gambles, then any residual credits or winnings are transferred back to the SSM.
- Gambles are made within the SPM 21 without the transfer of credit from the SSM. The credit account in the SSM is updated after a gamble and only then (for security) is the console informed of the gamble outcome. The SPM 21 may first check the SSM to verify enough credit is available to cover the bet or keep a record of the current credit available. This method eliminates the transfer of credit between SPM 21 and SSM and in the event of a power or communication failure the player retains their credit. A gamble that does not update the SSM has for all practical purposes not taken place.

A multiple smartcard implementation may be used in a system where gaming is only one of a range of applications (eg. telephone, electronic purse, EFTPOS, identification) provided on a multi-application smartcard. Typically the SSM is the multi-application smartcard held by the user. And the SPM is in the console into which the user inserts the smartcard. Security features of the SSM ensure access to the secure data is limited to authorised applications.

Initialisation

When the system is powered up, or an SGC is inserted into the console, communication is established between the SGC and console. The console interrogates 31 the SGC for its status, including results of initialisation diagnostics and the games (combinations) available for play and the SGC replies 32.

A game is constructed using an appropriate set of combinations from the SGC and game data which resides on the console. The console queries the SGC for its available combinations 31, 32 and determines from the available set of game data which games are possible. Referring to Figure 2, if more than one game is possible the player is presented with a choice of games and asked 33 to make a selection. The console then waits 34 for player input 35 before commencing game play 36. The SGC may contain combinations for which the console has no game data, and multiple sets of game data may exist for a single combination, not all of which reside on the console. Where the console is connected to a remote service, for example a game server, it may request a download of game data to its local store for

games that it would otherwise be unable to play. Download of code may be secured thought use of cryptographic techniques to prevent download of virus or other malicious code. The player will then be presented with an expanded choice of games available, the list of which is determined by:

- A list of the game data available from the server, stored locally on the console. The list may be updated periodically or on demand.
- The console sends to the server a list of the combinations available on the SGC. The server replies with the game data sets that it has that match the available combinations.

The console requests a download of game data for at least the selected game.

Game Play

Once the system has been initialised and the game selected the player is presented with the game screen, from which games are played and options changed. Figure 4 shows the sequence of events in playing a game.

Many games have options that can be adjusted, which for spinning reels or pseudo spinning reels games, typically include the number of lines to bet on, and the amount to bet on each line. The console waits 41 for player bet entry 42 and communicates the selected options to the SGC, which either accepts 43 or rejects the options according to its pre-programmed rules. These typically include maximum bet, maximum win, maximum total credits allowed, and other rules as may be required (by the jurisdiction or supplier). Only if the game parameters are correct may a game be played.

The console waits 44 for the player to press 'PLAY' 45 and then the console initiates a game 46 on the SGC, which generates a game outcome, updates its accounting 50, then informs the console of that outcome. The console then presents 47 the game and outcome to the player. After the game is completed and the outcome displayed 47, the console waits 48 for the next player input 49 and depending on whether the input is a command to play another game, or to change the bet amount, the console will progress to the 'wait for play' step 44, or the 'set amount bet' step 43. In one implementation the console need not wait for the game outcome before starting to display the game to the player, but it does not display the outcome until it is known from the SGC. For example the spinning game may start the reels spinning when the player presses play, prior to receiving the outcome, but not stop spinning the reels until the outcome is known.

In the event of power loss or other failure, the SGC must be able to resume game play at the point at which it left off. Therefore the game outcome and accounting are stored in E^2PROM, (which retains data during power loss) and must be updated before the result is communicated to the console to prevent tampering.

The game outcome includes:

- The credits won/lost.
- Anything accumulated over a number of games, eg. a standalone jackpot or points towards bonus features
- The parameters necessary for the display of the outcome to the player. For example, in a red/black double up the card colour, or in a spinning reel game the stopping positions of each of the reels.
- The state of the game. In a multiple part game it must be able to return to the same place as it left off.

Win and/or bet limits can be implemented. The limits may be set by the SGC, on a per game basis or downloaded to the card (perhaps via the same process used to transfer credit).

For ease of description, in the following discussion the term "accounting" refers to all parameters that must be updated per game, including the players financial information and other parameters as may be jurisdictionally required, such as credits in/out, total wins and turnover.

Accounting information must be updated in such as way that a partial update cannot be performed. If for example there are 10 items of accounting data per game, then all of the 10 items must be updated before the update is considered complete and the console informed of a result. Referring to Figure 3, one method of achieving this is to have at least two sets of accounting registers 51 - 55 and a separate index register 56 holding a value indicating which set holds the current account. An unused bank is completely updated before the index register is updated to select the new account register set, where 2 or more account sets are recorded, a game history can be maintained and reviewed or audited. In one implementation a hash, checksum or CRC on each register set and the index provides extra data security.

In the case that an E^2PROM memory location cannot be updated reliably when the power fails, neither retaining the original value nor correctly updating to the new value hence the index register is susceptible to errors.

Two methods of ensuring the index register can be updated correctly are:

- Gray coding the index register 56, such that as the index register increments from one account to the next only a single data bit changes. Any error affects only that bit and is not important. After reset the index register may be read and written to ensure that it contains a stable value.
- The index register 56 is repeated at least 3 times. Each instance is updated fully (ie with the correct write time) before the next is started, and the same write order is always maintained. A write error may only occur in one of the 3 locations, and the correct location is easily determined.

A common requirement on gaming machines is replay of previous games. Previous game outcomes and associated accounting information are stored in E^2PROM to the limit required and may also be stored on the console. Previous games may be replayed from either the console or SGC.

A common requirement on gaming machines is replay of previous games. Previous game outcomes and associated accounting information are stored in E^2PROM to the limit required and may also be stored on the console. Previous games may be replayed from either the console or SGC.

Random Number Generation

To ensure the game outcomes can never be predicted the random number sequence must be practically impossible to determine from outside the SPM.

The random number sequence problem can be approached in several ways, which may be used standalone or combined to further randomise the sequence:

- A cryptographically secure random number generator is used.
- A predetermined series of random numbers, or a quantity of predetermined random number seeds, are programmed into the SGC (SSM or SPM) by the casino each time credits are transferred or communication takes place. A limited number of random numbers are generated from each seed, before the next is used. When all of the random numbers or seeds have been used game play is suspended until the SGC again communicates with the casino. The sequence generated from each seed is thus too short to be analysed.
- A limit is placed on how fast the SPM may play games, to slow down an automated attack, such that it is fast enough for a player, but too slow to

analyse. It may for example be capable of 1000 games per second, but would be limited to only 2 per second.

- The SPM discloses only the outcome of the game, not the random number that was used to determine it. It is therefore more difficult to determine the random number, and hence sequence, as many different random numbers could have generated a particular outcome.
- A random number generator of sufficient complexity that it cannot be predicted.
- A sequence generated using a cryptographically strong hash function (eg MD5 or SHA) on a more easily predictable sequence, or similarly encrypting (eg DES or RSA) a more easily predictable sequence.
- A cryptographically secure pseudo-random number generator.
- The random number seed or algorithm might change in a predetermined sequence determined by the casino.
- Hardware support may be included on the smartcard to aid in the generation of true random numbers. For example thermal noise in electronic circuits is random and could be used to further randomise the sequence.
- Externally asynchronous events may be used to further randomise the sequence, for example the time between the playing consecutive games. This may only be used to further randomise an already pseudo-random sequence, as true asynchronous events cannot be guaranteed when tampering is taking place.
- Fake or zero value gambles may be made to test the SPM or educate the player about the games. When fake gambles are enabled the player's credit account is not updated with any wins or losses. A different random number seed and generator may be used for this mode to prevent automated tampering from trying to determine the random number sequence. Ideally, the fake generator would confuse any attempt at tampering for a long time.

When random sequences are determined externally, then to prevent tampering the sequences are generated by an authorised body and encrypted before use by the casino (the casino may be authorised). Many forms of encryption may be used, provided that only the SPM can decode or generate the messages. The casino can only pass the sequence on to the SPM, and could neither examine nor modify them.

The random numbers or seed may be stored as part of the game accounting and history to enable the replay of games.

In an alternate implementation instead of generating game outcomes from random numbers the SGC/SSM stores a list game of predetermined game outcomes. When all game outcomes have been used SGC cannot play more games until new game outcomes are loaded.

Transfer Of Credit

Credits are transferred between the SPM and/or SSM and casino using any suitable method including a similar or identical secure method as is done in a electronic cash system using smartcards

The player establishes an account with the casino and receives an SGC 11 or SSM, or if an SGC 11/SSM is already held, registers the SGC 11/SSM with the casino. Credit is transferred from the casino to the SGC/SSM for the player to gamble with. Credit held on the SGC/SSM can at any time be transferred back to the casino from the SGC/SSM at the request of the player and is credited back to the player's account.

When credit is transferred to the SGC 11/SSM and is gambled with by the player and the amount held increases or decreases according to the game outcomes. Only when the SGC 11/SSM communicates with the casino does the casino know the amount of credit on the smartcard. Therefore, to limit financial uncertainty the casino may place a time limit on the claiming of winnings stored on the SGC/SSM.

In one implementation, when credits are transferred to or from the SGC/SSM, the casino may build a history of transactions. The history would be analysed during each transaction to detect anomalous patterns which would indicate tampering, such as an unlikely win amount. During the credit transfer, the casino may also request the game history stored on the SGC 11/SSM to improve the analysis.

The SGC 11/SSM and/or the player's casino account may be anonymous or have the players name associated with it. Anonymous accounts have several advantages including privacy and tax considerations and enables cards to be traded or sold.

In one implementation of the system money may be transferred from one SGC 11/SSM to another, either indirectly through a transfer medium such as an interface unit, or directly where the cards communicate with each other via a simple interface. The SGC 11/SSM may not have a gamble

feature, or its use may be disabled, so that it is only used for the transfer of credit. In this instance it is similar or identical to other money carrying systems, and any such existing system may interface to the gaming system in this way. Security prevents replay attacks (in which a credit transfer is recorded and replayed to gain extra credit).

The player may collect money by direct transfer to their bank account, but as a security feature the casino may require the player to present their SGC 11 before payment is authorised. The SGC 11 can therefore be examined for tampering. In the event of a large win the SGC 11 may lock-up preventing further play and require the player to redeem the credit and possibly return the SGC 11, depending on the implementation preferred by the casino. The decision to require the SGC 11 to be returned may be random or depend on the amount of money to be collected.

Accounts

In one implementation a number of separate casinos may exist capable of transferring credit into the SGC 11 or SSM. Once a casino transfers credit onto the smartcard it may only be removed or added to by that casino and no other. This acts to prevent fraud and to keep the financial affairs of the companies separate. Each casino must be uniquely identified and unable to forge the identity of another. Therefore the SGC 11/SSM keeps an account holding the amount of credit in the SGC 11/SSM and the source of that credit. Credit from an account is gambled and any wins or losses associated with that gamble are credited or debited to that account. Identification and access to accounts may be controlled by cryptographic techniques to prevent unauthorised tampering with accounts.

The account ID may be either fixed or pre-programmed to work with one particular casino, or be capable of being changed depending on the requirements of the SGC 11/SSM provider and customer. To allow the account to be changed, once the account holds zero value the account ID is deleted, hence a new account may be established with another casino.

Multiple accounts may exist on the smartcard enabling the smartcard to be used by and with multiple casinos. Each account holds the amount of credit associated with that casino and is identified with the ID of the casino that provided it. Credit may only be transferred to or from an account by the casino that established the account, although that account may be deleted once there is zero balance.

The console 16 may query the SGC 11/SSM as to the account(s) ID and provide this information to the user. Where multiple accounts exist the player may be given the option of selecting the account on which to gamble, or the account may be selected by the SGC 11/SSM or console 16 depending on a scheme selected by the supplier.

In an application such as a traditional casino, with games played on the casinos console (which could appear to be traditional gaming machines), it is in the casinos interest to play only using the account held with that casino. If the SGC 11 is embedded within the console 16, or provided to the player by the casino, this is enforced by the programming of the SGC 11. However, if the SGC 11 is provided by the player and holds credit from another casino, then the casino might not gain from the player using its facilities.

Several methods may be used to alleviate this:

- The console would recognise that games were not being played using credit from the casino and refuse games.
- The casino arranges the transfer of credit via the console or other means, from the SGC 11 to the original casino, from the original casino to current casino, and back to the SGC 11. The credit is thus converted to that of the casino at which games are being played.
- The player adds credit to the smartcard in a separate account and only this account is gambled on.

In one implementation analysis software at the casino monitors the accumulated wins and losses associated with each smartcard for suspicious patterns which would represent an attempt to defraud. An unusually high rate of payout, for example. The data is collected each time a transfer of money is made between casino and SGC/SSM 11. When suspicious activity is detected the casino might refuse further business with that smartcard or customer, or carry out further investigations.

Communications

Communications between the SGC 11 and casino may be via the console or another means. For example, the console may be capable of communicating with the casino via Internet or by telephone. Alternatively, the SGC 11 may be removed from the console and plugged into a separate terminal to communicate with the casino.

Credit may be transferred to/from the smartcard via a 3rd party that simply acts as a mediator. SGC 11/SSM smartcards may be compatible with a bank or EFTPOS smartcard and be capable of interfacing with a bank ATM or shop point of sale equipment. Figure 5 shows an example where the casino 61 transfers credit to and from the SGC 11/SSM via an ATM 62 using a bank ATM network 63. Clearly other types of networks may be used. The transfer of credit is accomplished either directly between the casino 61 and SGC 11 with the 3rd party acting only as a communications medium, or credit being transferred first between SGC 11 and 3rd party, then the 3rd party and casino 61.

In the example of Figure 5 the ATM incorporates a SAM 14a, which communicates securely with the casino and SSM to enable the transfer of credit between casino and SSM. The SAM 14a/SSM keeps accounting and history information as required for auditing.

The SAM 14a may provide a secure means of reading and updating the SSM for many applications, of which the gaming application is only one or alternately multiple SAMs (or SPMs) may be integrated into a single console each providing a different application. Applications may be unrelated to gaming.

In an offline environment where communications between SAM and casino are intermittent the SAM may store a large number of gaming credits, smaller portions of which are transferred to and from the players SSM. Credits may therefore also be transferred between one SSM and another via the SAM.

Normally the casino performs conversion between credits and money, for which an on-line (to the casino) transaction is required. It is possible for the SAM to perform the transaction off-line, by accessing both accounts on the SSM and performing the appropriate conversion. When on-line communication with the bank and/or casino is re-established the appropriate transfer on money is made.

Security

The degree of security required from the SGC 11 is dependant on the threat against it and the SGC 11 may be constructed from components more or less secure than smartcards. However smartcards are relatively cheap and provide a high degree of security. It is recognised that smartcards may not be absolutely secure and with sufficient resources could be compromised.

Features of the system minimise the possible damage to an acceptable level, where the money gained is not worth the level of expenditure required.

In one implementation analysis software at the casino monitors the accumulated wins and losses associated with each smartcard for suspicious patterns representing an attempt to defraud. An unusually high rate of payout, for example. The data is collected each time a transfer of credit is made between casino and SGC. When suspicious activity is detected the casino might refuse further business with that smartcard or customer, or carry out further investigations.

In one implementation the casino may request the SGC be presented for inspection before payout, or at any other time. The SGC can then be examined for tampering. The SGC may carry additional means of identification, such a hologram or a magnetic stripe. Tamper resistant packaging may increase the likelihood of tampering being detected when the SGC is examined.

Where applicable the following general principals of cryptographic security will be applied:

1. All critical transmissions will be encrypted using state-of-the-art encryption scheme;
2. Key management schemes will be used to ensure security of keys;
3. The freshness of all transmissions will be ensured and monitored;
4. Mutual authentication of principals will be routinely implemented; and
5. Cryptographically strong, unbiased pseudo-random number generators will be used throughout the implementation.

License Protection

The SGC 11 is inherently protected against copying however the console 16 can also be protected against unlicensed manufacturing, such that only a licensed company can produce consoles.

Figure 6 illustrates the structure of the licensed console 16. The console 16 is fitted with a license card or chip 71, which is a variation of the SGC 11 with similar security attributes, preferably again a smartcard or smartcard chip. The SGC 11 securely communicates with the license card 71 and only plays games if it is present. Any manufacturer may make consoles, but a fee must be paid to obtain the license card 71 without which the SGC 11 will not play in that console 16.

In the preferred implementation of licensing the SGC 11 and license smartcard 71 use RSA encryption. All license smartcards 71 use the same encryption keys with the private key known only to the license smartcards 71 and the public key to the SGC 11. The SGC 11 generates a random number, encrypts it with the license smartcards public key, and sends it to the license smartcard 71 via the console 16. The license smartcard 71 decrypts the message with its private key and returns it to the SGC 11, which checks it against the original. Only a valid license smartcard 71 is able to decrypt the message and the SGC 11 is thus assured of the validity of the license. To prevent recording of the message a random number is used and is different each time.

Consoles may still be manufactured illegally but are useless without the licence smartcard. If removable cards are used then theses may be transferred from the original console to the new console without paying a new licence fee. However if a smartcard chip is used and is soldered directly to the printed circuit board in the console it cannot be easily removed.

Other asymmetric encryption algorithms may be used instead of RSA. Symmetric encryption may also be used, as the key is hidden within both the SGC and license chip.

Licence protection is also achieved in implementations which are varied from that shown in Figure 6 in that the embedded licence chip is replaced with an SGC and the removable SGC is replaced with an SSM.

Improved Traditional Gaming Machine

The invention may be used to enhance security within a traditional gaming machine. The security provided by a smartcard is far superior to that in a traditional gaming machine. The functions within the smartcard, including game combinations, accounting and game history cannot be tampered with.

In this implementation traditional machine security protects the physical smartcard, cash handling peripherals, communications, etc. The smartcard secures those functions within it. Only those functions not in the smartcard are susceptible to tampering. In a cashless system all the functions related to money and payout are within the smartcard, hence there is no benefit to be gained by tampering with the rest of the machine. Direct transfers of credit are made between the SGC 11 and the players SSM (eg. smartcard) or between SGC and host system via a network.

Auditing of the SGC can be either by inspection, the gaming machine itself, or via a network communications interface.

Traditionally download of code to the gaming machine has not been allowed because of the risk of tampering. The enhanced security of this implementation deters tampering, as it is either easily detected by audits or in a cashless system has no significant effect. An audit will detect tampering when the unalterable accounts in the SGC do not match the amount of money the machine holds. Code may be downloaded to the SGC when it is encrypted or digitally signed as described previously.

Progressives

A progressive system allows games or wins to trigger a chance to win in a pooled prize. Emulating this feature on the Personal Gaming System is enabled by recording the SGC the appropriate events and entering the player into the pooled prize gamble when communication between SGC and casino is made.

For example, a player gambles 200 times, winning 40 times. The SGC records that 40 wins were made and when communications is established with the casino the player is given 40 chances at the progressive prize.

The system is implemented in a similar way to a traditional progressive, the difference being that entries into the pool gamble are made periodically as communications with the casino is made, rather than in near real-time as gambles are being made.

Off-Line monitoring

Off-line monitoring enables government control and taxation of gambling machines.

The SGC is programmed with preset limits, which when reached disable further game play. The gaming machine containing the SGC is designed such that it is useless without the SGC and cannot be easily tampered with to enable its use. Therefore the government is assured that though its control of SGCs it controls gaming machines.

The data collected from the SGC enables gaming to be audited and taxes levied and allows the government strict control over gaming. Gambling by a particular player or at a particular establishment is easily stopped simply by not renewing SGCs as they reach the preset limit.

The pre-programmed limit is typically on the number of games played, amount gambled or collected. When play is disabled the player or operator

must return the SGC to a authorised monitoring agency for the stored data to be retrieved and game play re-enabled. Alternately secure communications between the SGC and authorised monitoring agency remove the need for physically presenting the SGC.

An agency is authorised to monitor and renew SGCs through the use of a device which can securely communicate with the SGC. Only an authorised device knows the encryption key required to communicate with the SGC, and hence only the authorised device can retrieve and clear the stored data. The authorised device may itself authorised for use with its own limits, on for example the number of SGCs it may enable. The authorised device may be implemented in at least two forms:

- A communication interface in which the SGC communicates with a remote gaming monitoring system. For example, if the SGC is a smartcard, a smartcard interface connected via a computer to a modem and hence to the remote monitoring system.
- An authorisation device containing an SGC interface. Encryption keys required to communicate with the SGC are securely stored within the device. Preferably the authorisation device contains at least a smartcard in which the encryptions key(s) are stored and encryption takes place.

Verification Mode

The SGC/SSM/SAM may be provided with a verification mode in which the memory contents of the device may be downloaded to an external device. Preferably in the interests of security, secret encryption keys (and optionally other sensitive data) stored within the SGC/SSM/SAM are not disclosed. Cryptographic techniques are used to ensure that only an authorised party is able to initiate the verification mode and the downloaded data may be encrypted to prevent disclosure. Preferably invocation of device verification disables the device from further use, except for device verification and minimal changes are made to the memory contents during this procedure.

It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive.

CLAIMS:

1. A game console secure control device implemented as a single secure integrated control circuit arranged to perform game outcome determination of a game played on a game console to which the control device is connected, the integrated control circuit having input/output means to allow communications with the console.

2. The game console secure control device as claimed in claim 1, wherein the secure control device includes a random number generating means or pseudo-random number generating means such that when a player playing the connected console initiates a game, a game outcome is generated by the secure control device making use of the random number generating means or pseudo-random number generating means.

3. The game console secure control device as claimed in any one of claims 1 or 2 wherein random number generation is performed within the secure control device and is by way of a random number generating means.

4. The game console secure control device of claim 3, wherein the random number generation employs a noise generating circuit.

5. The game console secure control device of claim 3, wherein the random number generation relies on the randomness of user input timing.

6. The game console secure control device of claim 3, wherein the random number generation employs a pseudo-random number generating algorithm.

7. The game console secure control device of claim 6, wherein one or more seeds are periodically loaded into the secure control device to break the pseudo-random sequence.

8. The game console secure control device as claimed in any one of the preceding claims wherein the secure control device is permanently or semi-permanently connected to the console.

9. The game console secure control device as claimed in any one of claims 1 to 7, wherein the secure control device is removably connectable to the console, whereby the player may possess the control circuit and insert it into a console of choice.

10. The game console secure control device as claimed in any one of the preceding claims wherein data storage means is provided within the secure control device and a credit balance associated with the player playing the game is stored in the data storage means.

11. The game console secure control device as claimed in any one of claims 1 to 9, wherein data storage means is provided within the secure control device and the data storage means is preprogrammed with a credit amount for use by the player to place wagers when playing the game, the secure control device being removably connectable to the console, whereby the player may possess the control circuit and insert it into a console of choice.

12. A game console secure control device implemented as a secure single integrated control circuit arranged to perform game outcome determination of a game played on a game console to which the control device is connected, the secure control device having data storage means and input/output means, the data storage means, including game outcome storage means whereby the control device is preprogrammed with a set of game outcomes in the game outcome storage means and when a player playing the connected console initiates a game, a game outcome is determined from the set of game outcomes and the input/output means being arranged to allow communication with the console.

13. The game console secure control device as claimed in any one of claims 1 to 9 or claim 12, wherein secure data storage means is provided externally to the integrated control circuit, the input/output means is arranged to provide secure communications with the data storage means.

14. The game console secure control device as claimed in claim 13 wherein a credit balance associated with the player playing the game is stored in the data storage means.

15. The game console secure control device as claimed in claim 13, or 14 wherein game combinations associated with the game being played are stored in the data storage means.

16. The game console secure control device as claimed in claim 13, 14, or 15 wherein programs associated with the games available for play on the console are stored in the data storage means.

17. The game console secure control device as claimed in claim 13, 14, 15, or 16 wherein predetermined game outcomes are stored in the data storage means.

18. The game console secure control device as claimed in claim 13, 14, 15, or 16 wherein predetermined random seed values for seeding a pseudo-random number generating algorithm are stored in the data storage means.

19. The game console secure control device as claimed in claim 13, 14, 15, or 16 wherein the data storage means is permanently or semi-permanently connected to the console.

20. The game console secure control device as claimed in claim 13, 14, 15, 16, 17 or 18 wherein the data storage means is removably connectable to the console, whereby the player may possess the data storage device and insert it into a console of choice.

21. The game console secure control device as claimed in claim 13, 14, 15, 16, 17 18, 19 or 20 wherein the secure communication is by way of cryptographic security means.

22. The game console secure control device as claimed in claim 13, 14, 15, 16, 17 18, 19 or 20 wherein the secure communication is by way of physical security means.

23. The game console secure control device as claimed in claim 13, 14, 15, 16, 17 18, 19, 20, 21, or 22 wherein the secure control device is permanently or semi-permanently connected to the console.

24. The game console secure control device as claimed in claim 13, 14, 15, 16, 17 18, 19, 20, 21, or 22 wherein the secure control device is removably connectable to the console, whereby the player may possess the control circuit and insert it into a console of choice.

25. The game console secure control device as claimed in any one of the preceding claims wherein the secure control device includes credit adjustment means arranged to adjust the credit balance associated with a player playing the game to account for a wager value associated with the game and, when a prize value is awarded as a result of the game, the prize value.

26. The game console secure control device as claimed in any one of claims 1 to 24 wherein the secure control device includes credit adjustment means arranged to adjust the credit balance associated with a player playing the game to deduct a wager from the credit balance and, when a prize value is awarded as a result of the game, crediting the prize value to the credit balance.

27. The game console secure control device as claimed in any one of claims 1 to 24 wherein the secure control device includes credit adjustment means arranged to adjust the credit balance associated with a player playing the game, the credit adjustment means being arranged to read the credit

balance, calculate a new balance and write the new balance to the data storage means.

28. The game console secure control device as claimed in any one of claims 1 to 24 wherein the secure control device includes credit adjustment means arranged to adjust the credit balance associated with a player playing the game, the credit adjustment means being arranged to communicate a credit balance adjustment amount to the data storage means, and the data storage means is arranged to calculate and store a new balance.

29. The game console control device as claimed in any one of the preceding claims wherein an outcome indication is produced by the console in response to a game outcome communicated by the control device, thereby indicating to the player the game outcome determined by the integrated control circuit.

30. The game console secure control device as claimed in any one of the preceding claims wherein the integrated control circuit is a data processing means having associated program storage means.

31. The game console secure control device as claimed in any one of the preceding claims wherein the program storage means includes a control program to control the playing of games on a gaming machine into which the secure control device is connected.

32. The game console secure control device as claimed in claim 31, wherein the control device is arranged to download the control program into the console to which it is connected during operation of the console.

33. The game console secure control device as claimed in any one of claims 1 to 32, wherein the integrated control circuit is a single integrated circuit.

34. The game console secure control device as claimed in any one of claims 1 to 32, wherein the integrated control circuit is a fixed function logic circuit.

35. The game console secure control device as claimed in any one of claims 1 to 33, wherein the integrated control circuit is a smartcard or a smartcard chip.

36. The game console secure control device as claimed in any one of claims 1 to 33 wherein the integrated control circuit is a smartcard chip mounted in a PCMCIA card.

37. The game console secure control device as claimed in any one of claims 1 to 33, wherein the integrated control circuit is a smartcard chip mounted in a custom card.

38. The game console secure control device as claimed in any one of claims 1 to 33, wherein the secure control device is a smartcard chip mounted in a floppy disk housing and provided with a magnetic interfacing means for communication with the heads of a floppy disk drive.

39. A game console secure control device as claimed in any one of the preceding claims, wherein the game outcome is arranged to be associated with any one of a plurality of game styles, each game style having a set of outcome indications including at least one indication corresponding to each different possible outcome.

40. The game console secure control device as claimed in any one of the preceding claims, wherein the secure control device is arranged to control each of a plurality of different game console types.

41. The game console secure control device as claimed in claim 40, wherein a common game is available for play on all of the plurality of console types.

42. A game console including outcome indication means and user input means, control means arranged to control the non-secure functions of the game console, and secure control device interface means to provide communication between the secure control device and the control means whereby, when the secure control device is present and the game console is in use, a game initiating input made by a player to initiate a game causes a game outcome to be determined by the secure control device and communicated to the console, the game outcome causing an outcome indication selected from a set of one or more possible indications to be exhibited by the outcome indication means.

43. The game console of claim 42, wherein secure data storage is provided in the console and is arranged to store a player credit balance of a player playing a game on the console, and the console further includes credit adjustment means arranged to adjust the credit to account for a wager value associated with the game and, when a prize value is awarded as a result of the game, the prize value.

44. The game console of claim 42 or 43, wherein the secure control device is a fixed function logic circuit.

45. The game console of claim 42 or 43, wherein the secure control device is a single integrated circuit.

46. The game console of claim 42 or 43, wherein the secure control device is a smartcard or a smartcard chip.

47. The game console of claim 42 or 43, wherein the secure control device is a smartcard chip mounted in a PCMCIA card.

48. The game console of claim 42 or 43, wherein the secure control device is a smartcard chip mounted in a custom card.

49. The game console as claimed in any one of claims 42 to 48, wherein game outcome indication is by voice messages.

50. The game console as claimed in any one of claims 42 to 49, wherein the outcome indication is a video image which is displayed on a video display device.

51. The game console as claimed in any one of claims 42 to 49, wherein the outcome indication is provided by a spinning reel display device.

52. The game console as claimed in any one of claims 42 to 51, wherein the game outcome is arranged to be associated with any one of a plurality of game styles, each game style having a set of outcome indications including at least one indication corresponding to each different possible outcome.

53. The game console of claim 52, wherein the selection between outcomes of equal prize value is made on a sequential basis.

54. The game console of claim 52, wherein the selection between outcomes of equal prize value is made on a random basis.

55. The game console as claimed in any one of claims 42 to 54, wherein the programs and screen definitions reside in non-secure memory in the game console, external to the secure control device.

56. The game console as claimed in any one of claims 42 to 54, wherein the secure control device is permanently or semi-permanently mounted in the console in a location that is not user accessible.

57. The game console as claimed in any one of claims 42 to 56, wherein the console is a freestanding gaming console housing.

58. The game console as claimed in any one of claims 42 to 56, wherein the console is a portable or hand held unit.

59. The game console as claimed in any one of claims 42 to 56, wherein the console is implemented as a personal computer with an interface to receive the secure control device.

60. The game console as claimed in any one of claims 42 to 56, wherein the console is implemented as a video game controller connected to a television.

61. The game console as claimed in any one of claims 42 to 56, wherein the console is implemented as an Internet access device with an interface to receive the game console secure control device.

62. The game console as claimed in any one of claims 56 to 61, wherein the program and data storage means include code and data respectively for generating user interface displays on a display device in the game console and for monitoring user input devices of the game console.

63. The game console as claimed in any one of claims 57 to 62, wherein the secure control device is a removable device carried by the user and is insertable into a game console of choice by the user.

64. The game console as claimed in any one of claims 56 to 63, wherein the game outcome determination is performed within the secure control device and is by way of a random number generating means

65. The game console of claim 64, wherein the random number generation employs a noise generating means.

66. The game console of claim 64, wherein the random number generation relies on the randomness of user input timing.

67. The game console of claim 64, wherein the random number generation employs a pseudo-random number generating algorithm.

68. The game console of claim 67, wherein one or more seeds are periodically loaded into the secure control device to break the pseudo-random sequence.

69. The game console as claimed in any one of claims 42 to 68, wherein the secure control device is arranged to control each of a plurality of different game console types.

70. The game console as claimed in claim 69, wherein a common game is available for play on all of the plurality of console types.

71. A method of verifying authorisation of a host device or system to use a program or preprogrammed device having a secure function which it performs when stored or located in or connected to the host device or system wherein the host device or system is provided with a secure authorisation device and the program or programmed device interrogates the authorisation device by transmitting or otherwise communicating a message to the

authorisation device and receiving a response from the authorisation device, determining, if the response corresponds with the original message, the authorisation device being passed as authentic and the program or programmed device being permitted proceed to perform its secure function only if this correspondence exists.

72. The method of claim 71, wherein the authorisation device is located in the console and used to authenticate a secure control device containing secure gaming functions and a credit balance.

73. A game console secure data storage means including a secure single integrated memory circuit arranged to be connected externally to a secure control device, the data storage means including game outcome storage means whereby the data storage means is preprogrammed with a set of game outcomes, the data storage means having input/output means arranged to provide secure communication with the integrated control circuit, such that when a player playing the connected console initiates a game, a game outcome is determined from the set of game outcomes.

74. The game console secure data storage means as claimed in claim 73, wherein the data storage means includes credit balance storage means whereby a credit balance associated with the player playing the game is stored in the data storage means.

75. The game console secure data storage means as claimed in claim 73 or 74, wherein the data storage means is permanently or semi-permanently connected to the console.

76. The game console secure data storage means as claimed in claim 73, 74 or 75, wherein the data storage means is removably connectable to the console, whereby the player may possess the data storage device and insert it into a console of choice.

77. The game console secure data storage means as claimed in claim 73, 74, 75 or 76, wherein the secure communication is by way of cryptographic security means.

78. The game console secure data storage means as claimed in claim 73, 74, 75 or 76, wherein the secure communication is by way of physical security means.

79. The game console secure data storage means as claimed in claim 73, 74, 75, 76, 77, or 78 wherein the secure control device includes credit adjustment means arranged to adjust the credit balance associated with a

player playing the game to account for a wager value associated with the game and, when a prize value is awarded as a result of the game, the prize value.

80. The game console secure data storage means as claimed in claim 79 wherein the credit adjustment means is arranged to read the credit balance, calculate a new balance and write the new balance to the data storage means.

81. The game console secure data storage means as claimed in claim 79 wherein the credit adjustment means is arranged to communicate a credit balance adjustment amount to the data storage means, and the data storage means is arranged to calculate and store a new balance.

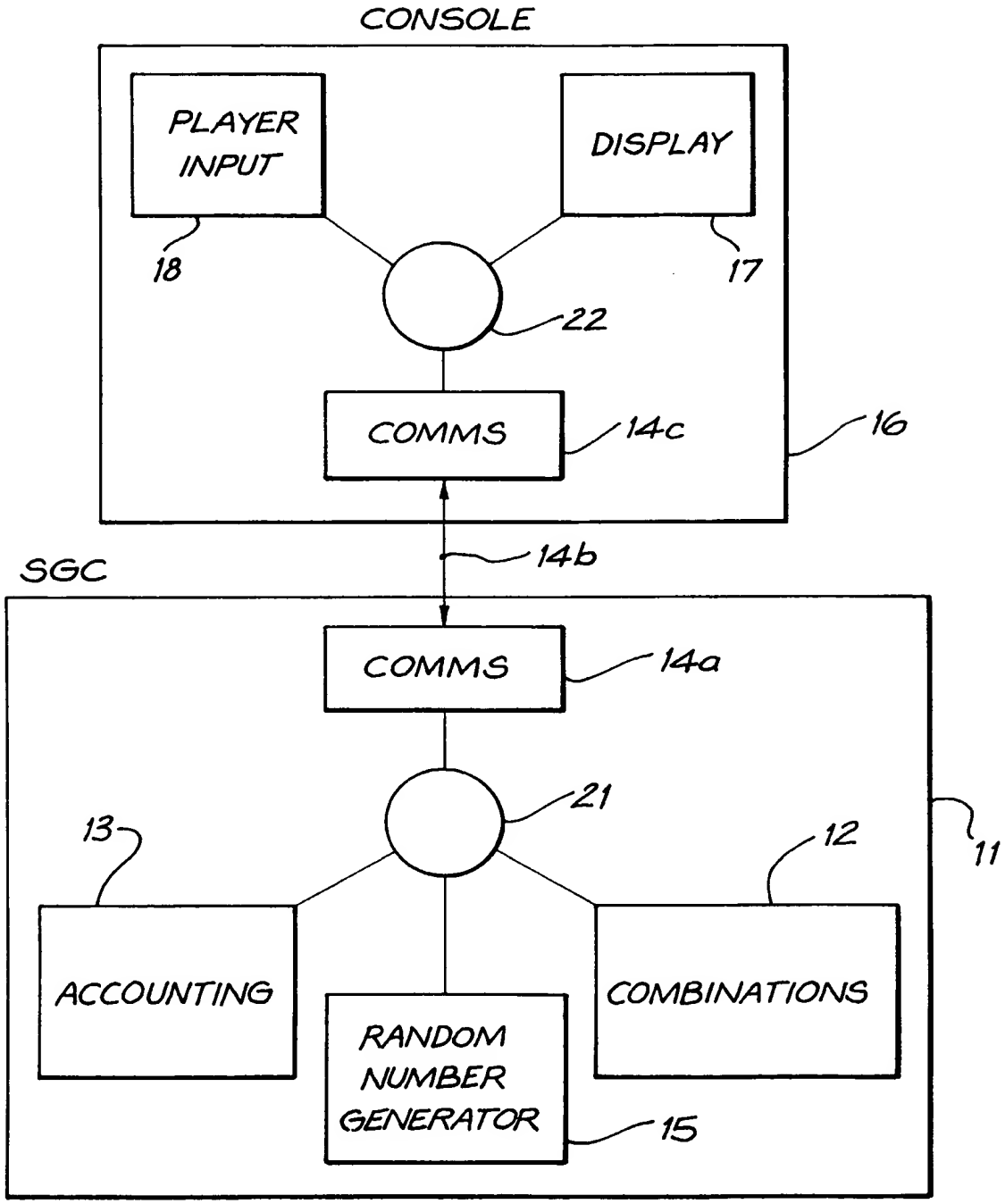

CONSOLE
PLAYER INPUT
DISPLAY
18
17
22
COMMS
14c
16
14b
SGC
COMMS
14a
21
13
12
11
ACCOUNTING
RANDOM NUMBER GENERATOR
15
COMBINATIONS

FIG. 1

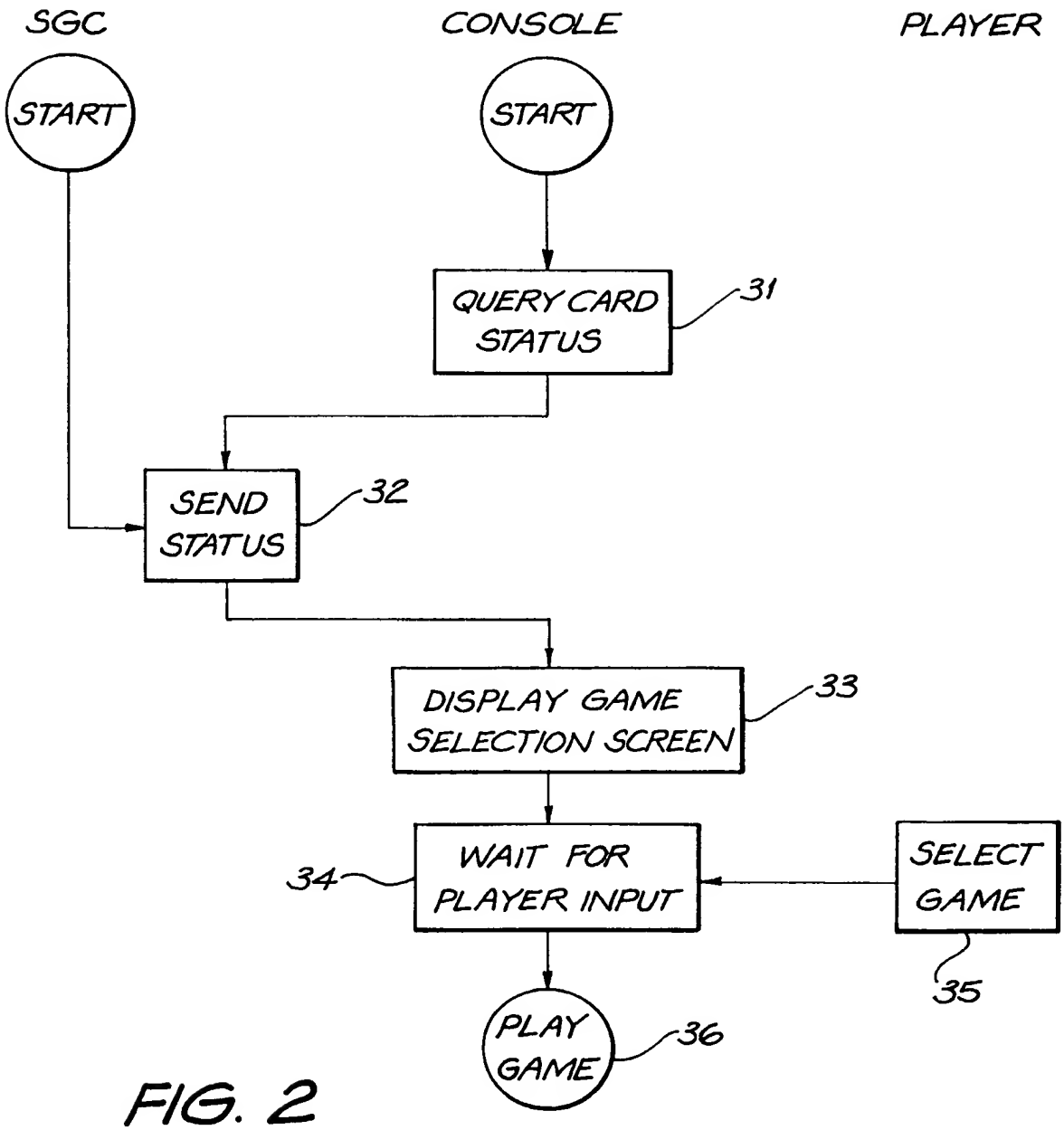

SGC
CONSOLE
PLAYER
START
START
QUERY CARD STATUS
31
SEND STATUS
32
DISPLAY GAME SELECTION SCREEN
33
WAIT FOR PLAYER INPUT
34
SELECT GAME
35
PLAY GAME
36

FIG. 2

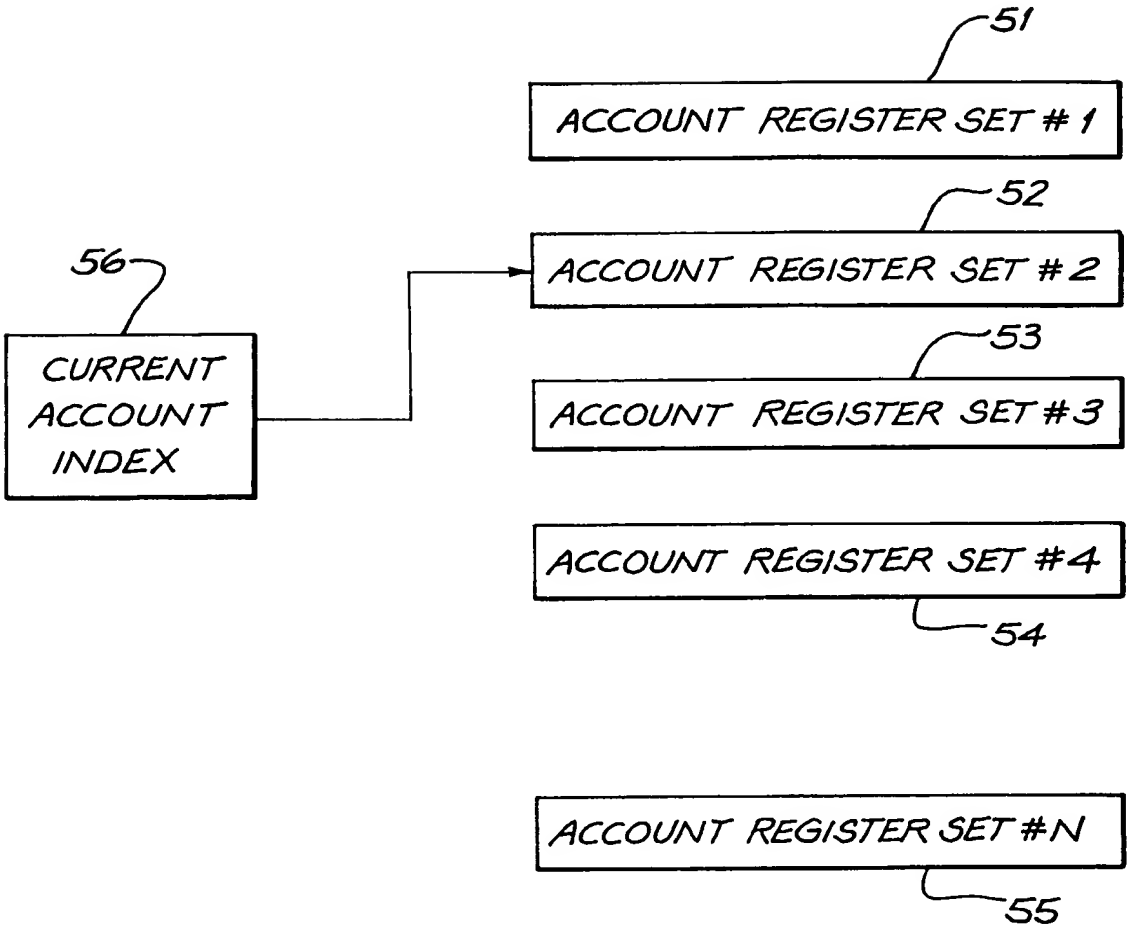

51
ACCOUNT REGISTER SET # 1
52
ACCOUNT REGISTER SET # 2
56
CURRENT ACCOUNT INDEX
53
ACCOUNT REGISTER SET # 3
ACCOUNT REGISTER SET # 4
54
ACCOUNT REGISTER SET # N
55

FIG. 3

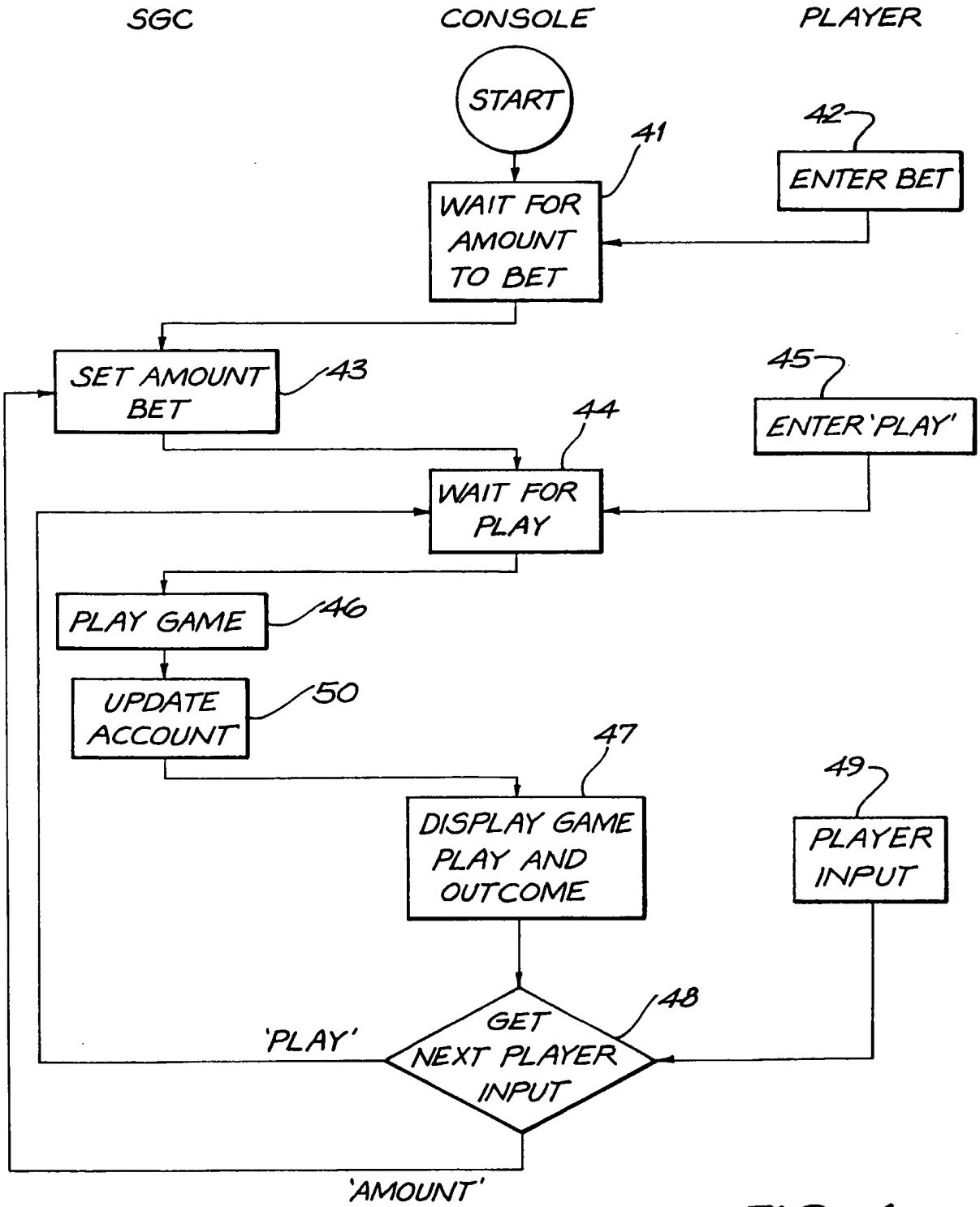

SGC
CONSOLE
PLAYER
START
41
42
ENTER BET
WAIT FOR AMOUNT TO BET
SET AMOUNT BET
43
45
ENTER 'PLAY'
44
WAIT FOR PLAY
PLAY GAME
46
UPDATE ACCOUNT
50
47
49
DISPLAY GAME PLAY AND OUTCOME
PLAYER INPUT
48
'PLAY'
GET NEXT PLAYER INPUT
'AMOUNT'

FIG. 4

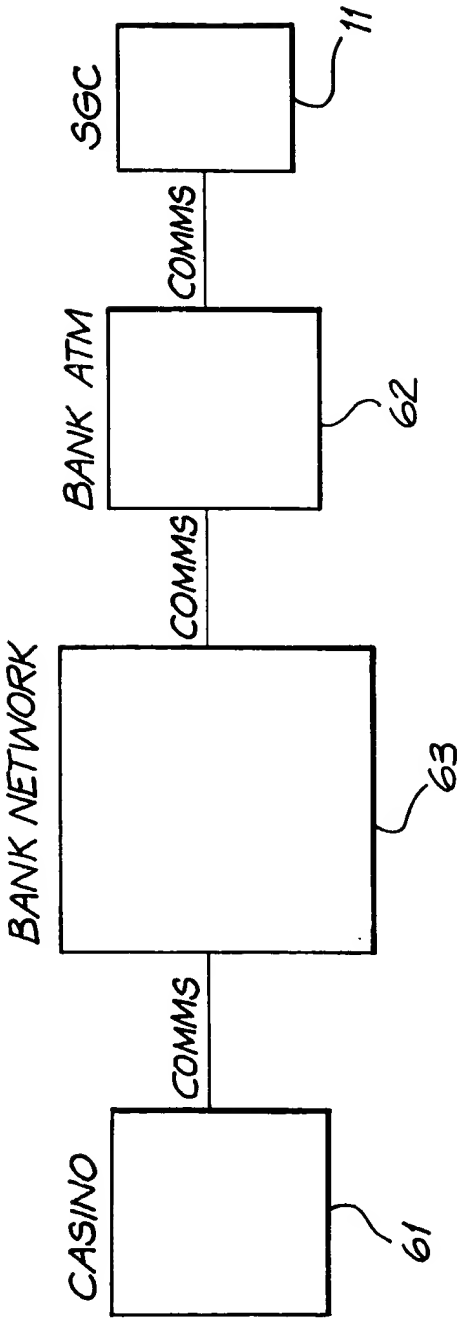

SGC
11
COMMS
BANK ATM
62
COMMS
BANK NETWORK
63
COMMS
CASINO
61

FIG. 5

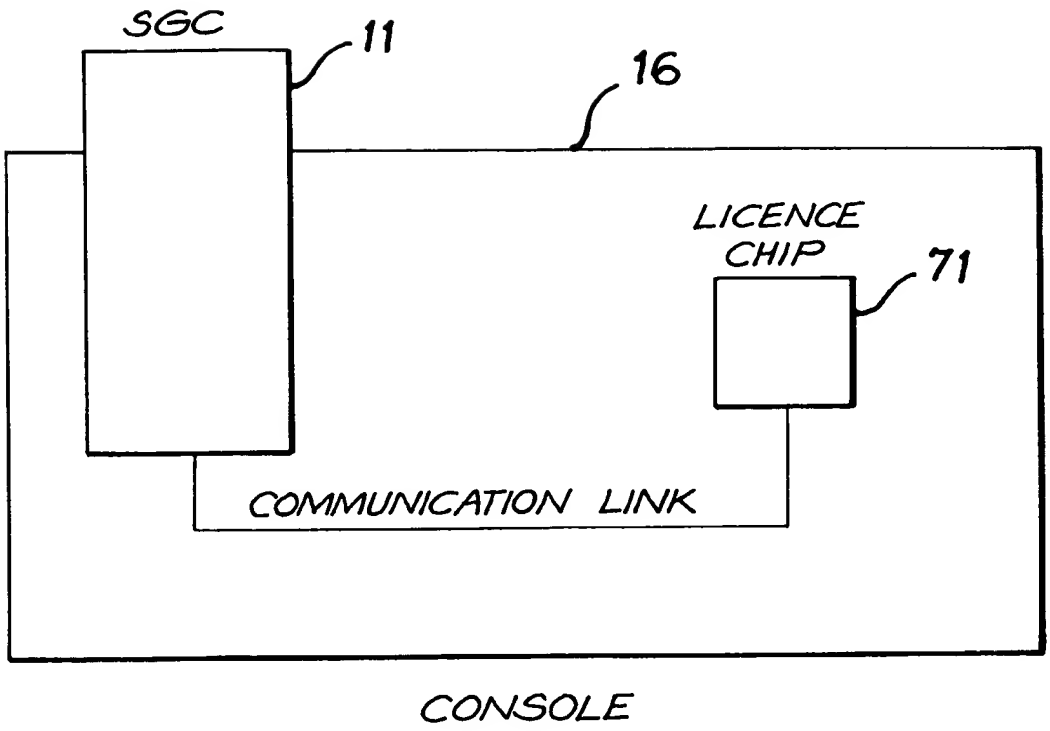


FIG. 6

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/AU 98/00152

A. CLASSIFICATION OF SUBJECT MATTER

Int Cl[6]: A63F 9/24 9/22, GO6F 161:00, G07F 17/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
A63F 9/24 9/22, G06F 161:00, GO7F 17/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
AU:IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
DERWENT: 1. GAM:AND SMART() CARD#
AND : 2. (AUTHOR: OR VERIF: OR AUTHENT:) AND (SMART() CARD# OR CARD#)
JAPIO: 3. (IPC as above) and (CONSOLE# OR SMART()CARD#)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	WO A 97/19428 (BROWN) 29 May 1997 See abstract, pages 2-4, page 7 lines 5-12 and figures 1 and 2.	1-70, 73-81
X	GB A 2287342 (WALKER) 13 September 1995 See abstract, pages 14-17 and figures 1A-1B and 13	1-70, 73-81

[X] Further documents are listed in the continuation of Box C

[X] See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
21 May 1998

Date of mailing of the international search report
27 MAY 1998

Name and mailing address of the ISA/AU
AUSTRALIAN PATENT OFFICE
PO BOX 200
WODEN ACT 2606
AUSTRALIA
Facsimile No.: (02) 6285 3929

Authorized officer
R Chao
Telephone No.: (02) 6283 2191

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/AU 98/00152

C (Continuation) **DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO A 92/10806 (GTECH CORP.) 25 June 1992 See abstract, pages 14-16 and figures 1-3	1-70, 73-81
X	US A 4764666 (BERGERON) 16 August 1988 See abstract, figures 3 and 9 and associated text	1-70, 73-81
X	JP A 09028900 (SOPHIA CO LTD) 4 February 1997 See abstract	71, 72
X	JP A 09024148 (SOPHIA CO LTD) 28 January 1997 See abstract	71-72
X	JP A 09050556 (SOFIA KK) 18 February 1997 See abstract	71-72
A	GB A 2298508 (BARCREST LTD) 4 September 1996 See abstract and figures 3	
A	WO A 97/02872 (CAESARS WORLD INC) 30 January 1997 See abstract and figure 6	

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/AU 98/00152

Box 1 Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a)

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. Claims 1-70 and 73-80 are directed to a game console secure control device.
2. Claims 71-72 are directed to verifying authorisation of a host device.

continued

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/AU 98/00152

Continuation of Box II

The International application does not comply with the requirements of unity of invention because if does not relate to one invention or a group of inventions so linked to form a single general inventive concept. It is considered that in the first group the game outcome determination and input/output communication means comprise a first "special technical feature" while in the second group the interrogation of the secure authorisation device comprise a second "special technical feature". Since the above mentioned groups of claims do not share either technical features identified, a "technical relationship" between the inventions, as defined in PCT rule 13.2 does not exist. Accordingly the International application does not relate to one invention as a single inventive concept.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International Application No.
PCT/AU 98/00152

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
WO	97/19428	AU	76325/96				
GB	2287342	AU	80254/94	BR	94/05271	CA	2137498
		CN	1122032	DE	4437277	DK	113/95
		FI	950950	FR	2717283	GB	2287342
		GR	95100048	HU	71560	IE	950162
		IT	95500164	JP	7255950	LU	88582
		MC	2402	NL	9402220	NO	950746
		OA	9971	PL	307582	PT	101671
		SE	9500437	SG	32319	WO	9524689
		AU	29531/95	WO	96/00950	ZA	9505451
WO	9210806	AU	91535/91	BR	9107145	MX	9102483
		OA	9782	US	5276312		92/10806
US	4764666	AU	22186/88	CA	1294052	EP	307925
GB	2298508	FR	2731288	GR	96/100066		96/100066
WO	97/02872	AU	63983/96	CA	2158523		

END OF ANNEX